Cloud Specific Terms and Definitions

(Terms appearing in the Taxonomy)
==========

First Level Terms:

1. Cloud Service Consumer - person or organization that maintains a business relationship with, and uses service from, Cloud Service Providers.

2. Cloud Service Provider – Person, organization or entity responsible for making a service available to service consumers.

3. Cloud Carrier – The intermediary that provides connectivity and transport of cloud services between Cloud Providers and Cloud Consumers.

4. Cloud Broker – An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between Cloud Providers and Cloud Consumers.

5. Cloud Auditor – A party that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation.

==========

Second Level Terms:

1. Cloud Distribution – The process of transporting cloud data between Cloud Providers and Cloud Consumers.

2. Cloud Access – To make contact with or gain access to Cloud Services.

3. Service Deployment – all of the activities and organization needed to make a cloud service available

4. Service Orchestration - refers to the arrangement, coordination and management of cloud infrastructure to provide different cloud services to meet IT and business requirements.

5. Cloud Service Management – Cloud Service Management includes all the service-related functions that are necessary for the management and operations of those services required by or proposed to customers.

6. Security – (See FISMA)

7. Privacy - Information privacy is the assured, proper, and consistent collection, processing, communication, use and disposition of disposition of personal information (PI) and personally-identifiable information (PII) throughout its life cycle. (Source: adapted from OASIS)

8. Software as a Service (SaaS) - The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating

systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. (Source: NIST CC Definition)

9. Platform as a Service (PaaS) - The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations. (Source: NIST CC Definition)

10. Infrastructure as a Sevice (IaaS) - The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls). (Source: NIST CC Definition)

11. Service Consumption – A Cloud Broker in the act of using a Cloud Service.

12. Service Provision – A Cloud Broker in the act of providing a Cloud Service.

13. Security Audit - Systematic evaluation of a cloud system by measuring how well it conforms to a set of established security criteria.

14. Privacy-Impact Audit - Systematic evaluation of a cloud system by measuring how well it conforms to a set of established privacy-impact criteria.

15. Performance Audit - Systematic evaluation of a cloud system by measuring how well it conforms to a set of established performance criteria.

==========

Third Level Terms:

16. Service Intermediation - An intermediation broker provides a service that directly enhances a given service delivered to one or more service consumers, essentially adding value on top of a given service to enhance some specific capability. (Source: Gartner)

17. Service Aggregation - An aggregation brokerage service combines multiple services into one or more new services. It will ensure that data is modeled across all component services and integrated as well as ensuring the movement and security of data between the service consumer and multiple providers. (Source: Gartner)

18. Service Arbitrage - Cloud service arbitrage is similar to cloud service aggregation. The difference between them is that the services being aggregated aren't fixed. Indeed the goal of arbitrage is to provide flexibility and opportunistic choices for the service aggregator, e.g., providing multiple e-mail services through one service provider or providing a credit-scoring service that checks multiple scoring agencies and selects the best score. (Source: Gartner)

19. Private Cloud - The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise. (Source: NIST CC Definition)

20. Community Cloud - The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise. (Source: NIST CC Definition)

21. Public Cloud - The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services. (Source: NIST CC Definition)

22. Hybrid Cloud – The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds). (Source: NIST CC Definition)

23. Service Layer - defines the basic services provided by cloud providers

24. Physical Resource Layer - includes all the physical resources used to provide cloud services

25. Resource Abstraction and Control Layer - Entails software elements, such as hypervisor, virtual machines, virtual data storage, and supporting software components, used to realize the infrastructure upon which a cloud service can be established

26. Portability - The ability to transfer data from one system to another without being required to recreate or reenter data descriptions or to modify significantly the application being transported. 2. The ability of software or of a system to run on more than one type or size of computer under more than one operating system. *See* POSIX. 3. Of equipment, the quality of being able to function normally while being conveyed. [Source: Federal Standard 1037C]

27. Interoperability - The capability to communicate, execute programs, or transfer data among various functional units under specified conditions. [Source: American National Standard Dictionary of Information Technology (ANSDIT)]

28. Provisioning/Configuration - process of preparing and equipping a cloud to allow it to provide (new) services to its users

29. Mobile Endpoints - A physical device, often carried by the user that provided a man/machine interface to cloud services and applications. A Mobile Endpoint may use multiple methods and protocols to connect to cloud services and applications.

30. Fixed Endpoints - A physical device, fixed in its location that provided a man/machine interface to cloud services and applications. A fixed endpoint typically uses one method and protocol to connect to cloud services and applications.

==========

Fourth Level Terms:

31. Data Portability – The ability to transfer data from one system to another without being required to recreate or reenter data descriptions or to modify significantly the application being transported. [Source: Federal Standard 1037C]

32. Service Interoperability - The capability to communicate, execute programs, or transfer data among various cloud services under specified conditions. [Source: modified from American National Standard Dictionary of Information Technology (ANSDIT)]

33. System Portability - The ability of a service to run on more than one type or size of cloud. [Source: modified from Federal Standard 1037C]

34. Rapid provisioning – Automatically deploying cloud system based on the requested service/resources/capabilities

35. Resource change – adjust configuration/resource assignment for repairs, upgrades, and joining new nodes into the cloud

36. Monitoring and Reporting – discover and monitor the virtual resources, monitor cloud operations and events, and generate performance reports.

37. Metering - provide a metering capability at some level of abstraction appropriate to the type of service (e.g, storage, processing, bandwidth, and active user accounts)

38. SLA management – encompasses the SLA contract definition (basic schema with the quality of service parameters), SLA monitoring, and SLA enforcement, according to the defined policies.

(Additional CC Terms not appearing in the Taxonomy but collected for completeness during the Taxonomy build activity)

==========

39. Service Requestor (OGSA) - This term is generally synonymous with client. In some contexts it may refer to a person, organization or higher-level system that makes use of a service offered by a service provider. (Source: Globus Alliance)

40. Resilience - the ability to reduce the magnitude and/or duration of disruptive events to critical infrastructure. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event. (Source: CRITICAL INFRASTRUCTURE RESILIENCE FINAL REPORT AND RECOMMENDATIONS, NATIONAL INFRASTRUCTURE ADVISORY COUNCIL, SEPTEMBER 8, 2009)

41. Resilience is the adaptive capability of an organization in a complex and changing environment. (Source: ASIS International, ASIS SPC.1-2009, American National Standard, Organizational

Resilience: Security, Preparedness, and Continuity Management System – Requirements with Guidance for Use.)

42. Reliability - A measure of the ability of a functional unit to perform a required function under given conditions for a given time interval. (Source: American National Standard Dictionary of Information Technology (ANSDIT))

43. Maintainability - A measure of the ease with which maintenance of a functional unit can be performed using prescribed procedures and resources. Synonymous with serviceability.

44. Usability - The extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use.

45. Cloud Subscriber - A person or organization that has been authenticated to a cloud and maintains a business relationship with a cloud. (Source: NIST SAJACC)

46. Cloud-subscriber-user - A user of a cloud-subscriber organization who will be consuming the cloud service provided by the cloud-provider as an end user. For example, an organization's email user who is using a SaaS email service the organization subscribes to would be a cloud-subscriber's user. (Source: NIST SAJACC)

47. Cloud-subscriber-administrator- An administrator type of user of a cloud-subscriber organization that performs (cloud) system related administration tasks for the cloud-subscriber organization. (Source: NIST SAJACC)

48. Cloud-user - A person who is authenticated to a cloud-provider but does not have a financial relationship with the cloud-provider. (Source: NIST SAJACC)

49. Cloud Service Developer – A person or entity engaged in the creation or improvement of cloud services or products

50. Authentication Credential - Something that an entity is, has, or knows that allows an entity to prove its identity to a system. (Source: NIST-SAJACC)

51. Cloud-subscriber - An authenticated person that accesses a cloud system over a network. A cloud-subscriber may possess administrative privileges, such as the ability to manage virtual machines, or the ability to regulate access by users to cloud resources the cloud-subscriber controls. (Source: NIST-SAJACC)

52. Data Object - A logical container of data, that can be accessed over a network. E.g., a blob. May be an archive, such as specified by the TAR format. (Source: NIST-SAJACC)

53. Physical Data Container - A storage device physically suitable for transferring data between cloud-subscribers and clouds. E.g., a hard disk. There has to be a standard format that the Provider supports (e.g., EIDE, IDE, SCSI). The physical data container must be formatted with a standard logical organization, such as FAT32, ufs, etc. (Source: NIST-SAJACC)

54. Provider - An organization that offers a network service that satisfies the definition of cloud computing given in Section (Source: NIST-SAJACC)

55. SLA - A document explaining expected quality of service and legal guarantees. (Source: NIST-SAJACC)

56. CloseDelay - the minimum latency, expressed in a common time unit, for a cloud provider to respond to a user's request to close an account. (Source: NIST-SAJACC)

57. User - A person or computer that accesses a cloud system over a network. A user may be authenticated but can also be anonymous. A user does not have administrative privileges on a cloud system. (Source: NIST-SAJACC)

58. FISMA compliant environment - an environment that meets the requirements of the Federal Information Security Management Act of 2002. Specifically, the law requires an inventory of information systems, the categorization of information and information systems according to risk level, security controls, a risk assessment, a system security plan, certification and accreditation of the system's controls, and continuous monitoring. [Source: Wikipedia]

59. Moderate impact - Moderate impact refers to the impact levels defined in FIPS 199. A potential impact is " moderate if the loss of confidentiality, integrity, and availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals." [IBID]

60. FedRAMP: FedRAMP allows joint authorizations and continuous security monitoring services for Government and Commercial cloud computing systems intended for multi-agency use. The use of this common security risk model provides a consistent baseline for Cloud based technologies and ensures that the benefits of cloud-based technologies are effectively integrated across a variety of cloud computing solutions. The risk model will enable the government to "approve once, and use often" by ensuring multiple agencies gain the benefit and insight of the FedRAMP's Authorization and access to service provider's authorization packages. (Source: Federal Risk and Authorization Management Program)

61. Virtualized Infrastructure Layer - Entails software elements, such as hypervisors, virtual machines, virtual data storage, and supporting middleware components used to realize the infrastructure upon which a computing platform can be established. While virtual machine technology is commonly used at this layer, other means of providing the necessary software abstractions are not precluded.

62. Facility Layer - Heating, ventilation, air conditioning (HVAC), power, communications, and other aspects of the physical plant comprise the lowest layer, the facility layer.

63. Hardware Layer - Includes computers (CPU, memory), network (router, firewall, switch, network link and interface) and storage components (hard disk), and other physical computing infrastructure elements.

64. Platform Architecture Layer - Entails compilers, libraries, utilities, and other software tools and development environments needed to implement applications.

65. Application Layer - Represents deployed software applications targeted towards end-user software clients or other programs, and made available via the cloud

66. Security Assessment - Assess the management, operational, and technical controls of the cloud system with frequency depending on risk, but no less than annually.

67. Security Certification - A security certification is conducted for accrediting the cloud system. The security certification is a key factor in all security accreditation (i.e., authorization) decisions and is integrated into and spans the system development life cycle.

68. Security Accreditation - The organization authorizes (i.e., accredits) the cloud system for processing before operations and updates the authorization or when there is a significant change to the system.